

En nationell strategi för samhällets informations- och cybersäkerhet

Regeringen presenterar en nationell strategi för hur informations- och cybersäkerheten i Sverige ska utvecklas och stärkas. Strategin sätter upp målsättningar inom sex prioriterade områden och ska bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt höja medvetenheten och kunskapen i hela samhället.

Digitaliseringen är ett globalt fenomen och påverkar i stort sett alla delar av vårt samhälle. Det medför stora möjligheter, men också risker. Allt från risker som enbart drabbar den enskilde individen, till välplanerade och riktade angrepp mot centrala samhällsfunktioner. Hur vi hanterar riskerna som följer av digitaliseringen har stor betydelse för vår förmåga att upprätthålla och stärka både vårt välbefinnande och vår säkerhet.

Strategin för samhällets informations- och cybersäkerhet har sin utgångspunkt i målen för Sveriges säkerhet: att värna befolkningens liv och hälsa, liksom samhällets funktionalitet, samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter¹. Strategin har även sin utgångspunkt i det it-politiska målet att

Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter².

Sex strategiska prioriteringar

För att främja målen för Sveriges säkerhet och it-politik bedömer regeringen att det framför allt är sex områden inom samhällets informations- och cybersäkerhet som behöver prioriteras.

Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

Informations- och cybersäkerhet angår hela samhället och alla behöver ta sitt ansvar. Samverkan och informationsdelning på informations- och cybersäkerhetsområdet behöver därför stärkas, och förutsättningarna för att bedriva ett systematiskt informationssäkerhetsarbete på ett mer enhet-

ligt och samordnat sätt behöver förbättras.

Öka säkerheten i nätverk, produkter och system

Samhället är i dag beroende av elektroniska kommunikationer och dessa måste därför vara effektiva, säkra och robusta samtidigt som de tillgodoser användarnas behov. Tillgången till säkra kryptosystem för it- och kommunikationslösningar måste också motsvara behoven i samhället och det krävs en ökad säkerhet i industriella informations- och styrsystem som t.ex. styr och övervakar el-distribution och dricksvattenförsörjning.

Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter

För att kunna minska konsekvenserna av cyberattacker och andra it-incidenter krävs såväl

ökad samverkan och planering som adekvata tekniska hjälpmedel. För Sveriges mest skyddsvärda verksamheter, inklusive sådana system som är vitala för totalförsvaret, ska det finnas ett utvecklat cyberförsvar med en förstärkt militär förmåga att möta och hantera angrepp från kvalificerade motståndare i cyberrymden.

Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet

Antalet anmälda it-relaterade brott ökar kraftigt. Förmågan att förebygga och bekämpa dessa brott måste stärkas genom en anpassad lagstiftning, utvecklad kompetens och organisation samt ett förstärkt internationellt samarbete. Fler aktörer utöver de brottsbekämpande

myndigheterna behöver därutöver aktivt delta i det förebyggande arbetet.

Öka kunskapen och främja kompetensutvecklingen

För att kunna fokusera på de mest angelägna säkerhetsbehoven behövs ökad kunskap och fler kartläggningar av informationssäkerheten i samhället. Såväl högre utbildning, forskning och utveckling som regelbunden övningsverksamhet är också av avgörande betydelse på detta område.

Stärka det internationella samarbetet

Vi är inte ensamma om att möta utmaningarna inom informations- och cybersäkerhet. Internationella samarbeten kring cybersäkerhet, både inom EU och

i andra internationella organ, behöver stärkas inom ramen för målsättningen om ett globalt, tillgängligt, öppet och robust internet som präglas av frihet och respekt för mänskliga rättigheter.

Uppföljning av strategin

Strategin kommer att följas av specifika uppdrag till berörda myndigheter för att målsättningarna ska kunna nås. Teknik- och hotutvecklingen innebär att informations- och cybersäkerhetsområdet förändras och utvecklas i snabb takt. Strategin måste därför ha en flexibilitet att kunna anpassas till de snabba omvärldsförändringarna och är därför inte tidssatt. Regeringen kommer att prioritera genomförandet av strategin och noggrant bevaka hur området utvecklas.

1. prop. 2008/09:140,
bet. 2008/09:FöU10,
rskr. 2008/09:292
2. prop. 2011/12:1,
bet. 2011/12:TU1,
rskr. 2011/12:87

Produktion: Justitiedepartementet
www.regeringen.se/justitie